Enabling key management in conjunction with encryption had a minimal performance impact on baseline IOPS, latency, and throughput

HCI cluster performance scaled linearly

Transitioning from iLKM to SEKM was simple

Protect data at rest with negligible impact on NVMe disk performance metrics

by enabling Secure Enterprise Key Manager on Dell PowerEdge servers

Cybercrime is on the rise and in the news—with huge costs to organizations that lose control of their customers' data. In fact, according to an annual report published on July 27, 2022, the average cost of a data breach this year was $4.4 million.[1]

The Dell™ PowerEdge™ Secure Enterprise Key Manager (SEKM) feature available on new Dell PowerEdge servers provides additional data security with full disk AES-256 encryption and external key management.

While disk encryption and effective key management are cornerstones to any comprehensive data protection strategy, some IT admins may assume that server storage performance is an associated casualty. To determine how disk performance changed after enabling the SEKM feature, we set up a hyper-converged infrastructure (HCI) cluster consisting of three Dell PowerEdge R7525 servers in 2- and 3-NVMe® disk group configurations. Then, we captured HCIBench performance metrics twice on each configuration: first without SEKM and then with SEKM. We found that enabling hardware-based data encryption with key management had a minimal performance impact on baseline IOPS, latency, and throughput results. Additionally, HCI cluster performance scaled linearly when we added storage. We also verified on a Dell PowerEdge R750xs server that transitioning from iDRAC LKM (iLKM) to SEKM took under three minutes/14 steps.

Prevention is the best medicine

A comprehensive data protection strategy must account for growth of data within the business, increasing privacy regulations, and the risk of data breaches and hacking—and also includes strict controls for overall resilience. The penalties for non-compliance can be onerous.

For example, according to the Global Data Privacy & Security Handbook, organizations failing to protect information on a single United States citizen can result in fines from the U.S. Department of Health and Human Services (HHS) and the Federal Trade Commission (FTC), in addition to other penalties, which could include imprisonment in state-specific instances.[2]

Inadequate security measures can put enterprise data in the crosshairs of sophisticated cyberattacks and hackers operating both inside and outside the organization. Data breach experts estimate that 95 percent of cyber security breaches occur because of human error.[3] A solid knowledge of which data needs protecting, a zero-trust approach, and encryption along with key management can go a long way to keeping sensitive data safe.

Data-at-rest security threats

Government regulations and industry associations have strict rules in place to protect personally identifiable information (PII), protected health information (PHI), and financial information.

Infrastructure in uncontrolled places, such as edge environments and colocation sites, is vulnerable to physical tampering and removal. End-of-life disposal is also a concern if a decommissioning process does not follow stringent security protocols.

Protecting data at rest

The combination of the costs of someone getting at insecure data and the potential penalties for violating those regulations combine to make insecurity a big issue. While data can be exposed in transit, data at rest is particularly vulnerable because the greater volume of information makes it very attractive to attackers.[4]

How Secure Enterprise Key Manager can improve data security

SEKM is a key management solution that uses best practice of isolating keys away from the storage location.[5]

With SEKM, authorized admins use an external key management service (KMS), such as Thales CipherTrust Manager, to store and manage encryption keys. This creates an extra layer of protection for sensitive data. SEKM, through the iDRAC, enables key exchange between the external key manager to server resident drives including direct-attach NVMe drives in addition to traditional drive configurations.[6]

LKM, iLKM, and SEKM

Encryption keys are often targeted by cybercriminals, which makes the proper management of those keys a primary concern for organizations.[7] SEKM, by storing the keys away from the local storage, is the strongest of the three solutions.

Local key management (LKM) is a standard PERC feature that requires no additional licensing or hardware. This budget option stores the key in the PERC RAID Controller and uses pass-phrases to manage access.

Integrated LKM (iLKM*) is IDRAC-based and enables key exchange locally. This is particularly useful on direct-attach NVMe configurations where a PERC RAID controller is not available.

SEKM* uses a KMIP compliant element in the iDRAC to securely connect to an upstream key management server. This centralizes key management away from encrypted drives, which insures that the data at rest within compromised drives is inaccessible.

*Requires SEKM license.

What we tested

To measure disk performance scalability, we set up an HCI cluster consisting of three Dell PowerEdge R7525 servers, first in a 2-NVMe disk group configuration and again in a 3-NVMe disk group configuration. We captured baseline HCIBench performance metrics on both disk group configurations. We compared the IOPS, latency, and throughput results to ones we obtained after enabling the SEKM feature and rerunning the tests. We found that the Dell PowerEdge R7525 cluster had almost the same results with SEKM enabled through Thales CipherTrust Manager, our KMS provider, as the same cluster without the added data security.

We also deployed an SEKM-enabled environment on a Dell PowerEdge R750xs server to do the following:

1. Confirm the ability to secure an NVMe drive in real time, pre-boot
2. Demonstrate the ease of the encryption migration path in two ways:
    a. Measure the time and steps to transition from an LKM-enabled iDRAC PERC (physical disks and RAID controller) to an SEKM-enabled iDRAC PERC
    b. Measure the time and steps to transition from iDRAC-native LKM to iDRAC-native SEKM using NVMe drives

For detailed system configuration information, benchmark parameters, and a step-by-step testing methodology, see the science behind the report.

Current-generation Dell PowerEdge servers

To support the most challenging data-intensive workloads, Dell PowerEdge servers now feature PCIe® Gen 4.0 technology and up to six accelerators per server.[8] But, with that power comes much responsibility—especially for data at rest. That is why Dell "enhanced security and cyber-resilient innovations protect servers through their full lifecycle."[9]

Enabling hardware-based security

As the demand for real-time and personalized customer interactions fuels the need for speedy response times and advanced analytics insights, the increasing amount of sensitive data increases data breach stakes exponentially. Software-based encryption is tempting for businesses on a tight budget, but it doesn't help if someone loses or steals physical systems, such as servers.

Additionally, hardware-based encryption with external key management might make more sense for financial, healthcare, and government sectors—where, according to the Dynamic Solutions Group®, "[r]egulations such as the Health Insurance Portability and Accountability Act (HIPAA) and Payment Card Industry Data Security Standard (PCI DSS) often have strict requirements regarding encryption of sensitive information. By complying with these regulations by using strong encrypted devices, your business can avoid expensive fines, lawsuits, and reputational damage."[10]

Choosing hardware-based encryption with external key management does not have to mean hurting the performance of systems running critical workloads. To examine the system performance impact of enabling SEKM, we first ran 4KB random read and 4KB random read/write workloads on two disk group configurations (with 12 and 16 NVMe drives) on Dell PowerEdge R7525 servers without SEKM in a cluster. Then, we enabled the SEKM feature on the same servers in the cluster and ran the same two workloads on the 2- and 3-NVMe disk group configurations. The IOPS, latency, and throughput numbers here show the median of three runs.

In both disk group configurations, the cluster of PowerEdge R7525 servers with and without SEKM performed comparably.

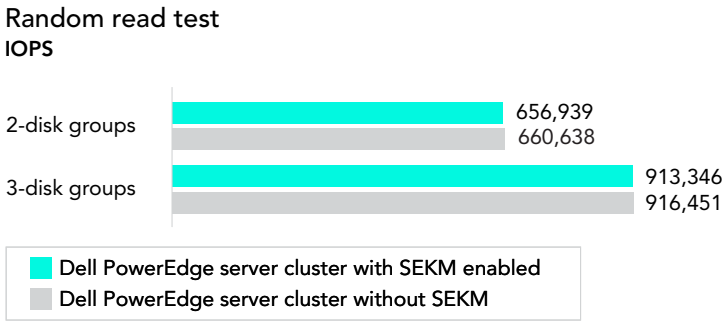

Figure 1: Random read HCIBench IOPS results with 12 and 16 NVMe drives in an HCI cluster consisting of three Dell PowerEdge R7525 servers. Higher is better. Source: Principled Technologies.

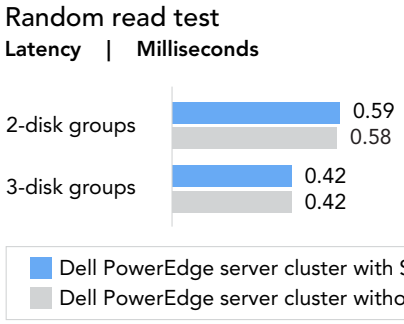

Figure 2: Random read HCIBench latency results with 12 and 16 NVMe drives in an HCI cluster consisting of three Dell PowerEdge R7525 servers. Lower is better. Source: Principled Technologies.

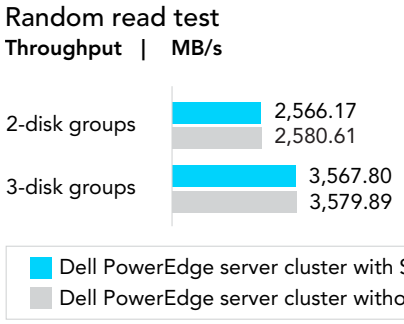

Figure 3: Random read HCIBench throughput results with 12 and 16 NVMe drives in an HCI cluster consisting of three Dell PowerEdge R7525 servers. Higher is better. Source: Principled Technologies.

Random read/write test
IOPS

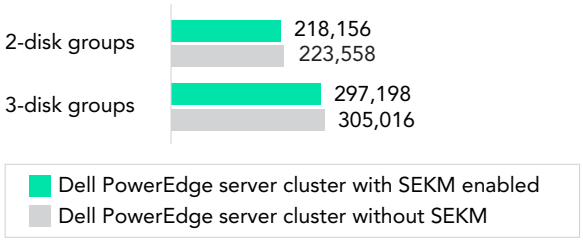

Figure 4: Random read/write HCIBench IOPS results with 12 and 16 NVMe drives in an HCI cluster consisting of three Dell PowerEdge R7525 servers. Higher is better. Source: Principled Technologies.

Random read/write test
Latency | Milliseconds

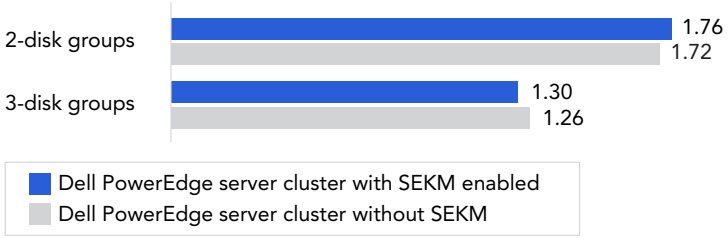

Figure 5: Random read/write HCIBench latency results with 12 and 16 NVMe drives in an HCI cluster consisting of three Dell PowerEdge R7525 servers. Lower is better. Source: Principled Technologies.

Random read/write test
Throughput | MB/s

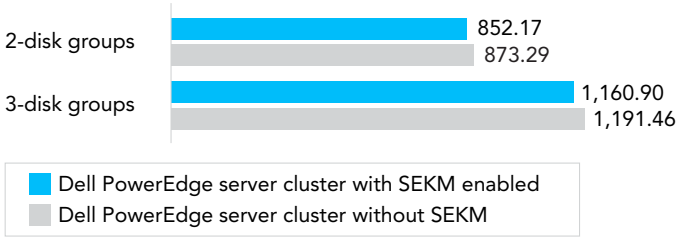

Figure 6: Random read/write HCIBench throughput results with 12 and 16 NVMe drives in an HCI cluster consisting of three Dell PowerEdge R7525 servers. Higher is better. Source: Principled Technologies.

Thales CipherTrust Manager

With the SEKM feature, companies can generate, manage, and store keys away from the data at rest. Thales CipherTrust Manager (the KMS we used in testing) adds an extra layer of security by "enabling organizations to centrally manage encryption keys, provide granular access control and configure security policies."[11] If the power goes down (or someone moves the drives), the drives lock, and the iDRAC retrieves the keys from the KMS to unlock the drives to continue. For more information about Secure Enterprise Key Manager and Thales CipherTrust Manager, read the Dell Technologies "Data Security for PowerEdge Servers Made Easy" blog post: https://www.dell.com/en-us/dt/solutions/openmanage/secure-enterprise-key-manager.htm#accordion0.

Real-world benefits of SEKM security

There are many scenarios where enabling the SEKM feature can help your company secure and retrieve data at rest. If a bad actor steals your drives, the SEKM solution prevents them from accessing the data from a different system. But what about more common, less nefarious scenarios? These could include times when the system loses power, or the drives lock. In these instances, the iDRAC simply retrieves the keys to unlock the drives from the KMS and the data is then available. The SEKM design also allows for flexibility and drive movement. For instance, when you migrate drives to another server in the same security group, the SEKM solution will recognize the drive and fetch the appropriate key from the KMS. However, the SEKM feature blocks key access if you move the drive to a server in a different security group or outside the data center.

For SAS configurations, iDRAC retrieves the key and uses the PERC for key exchange. In cases where NVMe drives are directly attached to the CPU, iDRAC can exchange keys with the drives directly. Additionally, there is no penalty to adding new disk groups, SEKM manages self-encrypting drives through iDRAC, and the feature regulates the self-encrypting drives with encryption at rest. The real-world benefits illustrated below reflect our hands-on evaluation of the SEKM solution in these scenarios on a Dell PowerEdge R750xs server.

SEKM advantages

» SEKM does not keep the drive-unlocking keys (KEK keys) on the server.

» An external KMS partner provides centralized key management for SEKM.

» SEKM supports the Key Management Interoperability Protocol (KMIP)—enabling a standards-based approach to key management.[12]

We used the iDRAC to manage both direct-attached NVMe and PERC-attached SAS SEDs.

Simultaneously secure NVMe and SAS SED drives.

Seamlessly change security type.

We switched from iDRAC LKM to SEKM in under 3 minutes/14 steps.

We configured SEKM direct-attached encryption in under 2.5 minutes/13 steps.

Quickly enable SEKM direct-attached encryption.

Rebootlessly update drive firmware through the iDRAC.

We enabled firmware updates with no downtime.

Conclusion

Our results show that, after incorporating the extra layer of data security afforded by the Secure Enterprise Key Manager solution on an HCI cluster of Dell PowerEdge R7525 servers configured with 2- or 3-NVMe disk groups, the HCIBench benchmark recorded IOPS-based performance metrics that were comparable to our baseline test results. We also found that incorporating the extra layer of hardware-based data security on a Dell PowerEdge R750xs server required minimal transition effort.

1. Dark Reading, "Average Data Breach Costs Soar to $4.4M in 2022," accessed August 15, 2022, https://www.darkreading.com/risk/most-companies-pass-on-breach-costs-to-customers.
2. Global Data Privacy & Security Handbook,"Penalties for Non-compliance - United States," accessed August 16, 2022, https://resourcehub.bakermckenzie.com/en/resources/data-privacy-security/north-america/united-states/topics/penalties-for-non-compliance.
3. CyberTalk.org, "Alarming cyber security facts to know for 2021 and beyond," accessed August 16, 2022, https://www.cybertalk.org/2021/12/02/alarming-cyber-security-facts-to-know-for-2021-and-beyond/.
4. Endpoint Protector, "How to Protect Your Data at Rest," accessed August 16, 2022, https://www.endpointprotector.com/blog/how-to-protect-your-data-at-rest/.
5. Dell Technologies, "Dell OpenManage Secure Enterprise Key Manager," accessed June 30, 2022, https://www.dell.com/en-us/dt/solutions/openmanage/secure-enterprise-key-manager.htm#accordion0.
6. Dell Technologies, "Dell OpenManage Secure Enterprise Key Manager."
7. Techopedia, "10 Best Practices for Encryption Key Management," accessed October 19, 2022, https://www.techopedia.com/2/30767/security/10-best-practices-for-encryption-key-management-and-data-security.
8. Dell Technologies, "Dell Technologies Powers AI and Edge Computing with Next Generation PowerEdge Servers," accessed June 30, 2022, https://www.dell.com/en-us/dt/corporate/newsroom/announcements/detailpage.press-releases~usa~2021~03~20210317-dell-technologies-powers-ai-and-edge-computing-with-next-generation-poweredge-servers.htm#/filter-on/Country:en-us.
9. Dell Technologies, "Dell Technologies Powers AI and Edge Computing with Next Generation PowerEdge Servers."
10. Dynamic Solutions Group, "Software vs. Hardware Encryption: The Pros and Cons," accessed July 1, 2022, https://www.dsolutionsgroup.com/software-vs-hardware-encryption/.
11. Thales, "Next Generation Enterprise Key Management," accessed August 19, 2022, https://cpl.thalesgroup.com/encryption/ciphertrust-manager.
12. Dell Technologies, "Enable OpenManage Secure Enterprise Key Manager (SEKM) on Dell EMC PowerEdge Servers," accessed June 30, 2022, https://downloads.dell.com/manuals/common/dell-emc-enable-openmanage-sekm-poweredge.pdf.

Read the science behind this report at https://facts.pt/uyQUM18 ▶

Principled Technologies®

Facts matter.®

This project was commissioned by Dell Technologies.